

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

TYRONE BANKS, individually and on behalf of
all others similarly
situated,

Plaintiff,

v.

FRESENIUS VASCULAR CARE, INC.
d/b/a AZURA VASCULAR CARE, INC.

Defendant.

Case No.

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Tyrone Banks (“Plaintiff”) brings this Class Action Complaint against Defendant Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care, Inc. (“Azura” or “Defendant”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to his own actions and their counsels’ investigations, and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action lawsuit against Azura for its failure to properly secure and to safeguard the personally identifiable information (“PII”) and protected health information (“PHI”) of hundreds of thousands of people.

2. Beginning at least as early as September 27, 2023, the sensitive patient medical data with which Azura had been entrusted was compromised in a cybersecurity incident (the “Data Breach”). A subsequent investigation undertaken on behalf of Azura revealed that the “attacker(s) accessed certain systems and encrypted certain files” which “included personal information for

some of our patients.”¹

3. Azura has acknowledged that the compromised data included names, mailing addresses, birthdates, Social Security numbers, unspecified “diagnosis and treatment information,” and other medical information.² The breach also impacted similar information – also entrusted to Azura – of certain “account guarantors.”

4. All-in-all, the Data Breach has reportedly impacted approximately 348,000 patients.³ Inexplicably, many of these people are just receiving letters (dated January 12, 2024) for an incident that first occurred in September of 2023, and which was initially discovered by Azura in November of 2023.

5. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Azura’s inadequate safeguarding of Class Members’ Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and Class Members.

PARTIES

6. Plaintiff Tyrone Banks at all relevant times was and is a resident of Chicago, Illinois.

7. Defendant Fresenius Vascular Care, Inc. d/b/a Azura Vascular Care, Inc. is a company with its principal place of business located at 40 Valley Stream Parkway, Malvern, PA 19335 It was formed by and is a wholly owned business unit of Fresenius Medical Care Holdings,

¹ *Id.*

² *Id.*

³ *Azura Vascular Care reports data breach, exposing 348k patients*, (Feb. 7, 2024), available: https://beyondmachines.net/event_details/azura-vascular-care-reports-data-breach-exposing-348k-patients-v-y-m-o-9.

Inc., a limited partnership organized under the laws of New York corporation and does business as “Fresenius Medical Care North America.” Azura operates 70 outpatient clinics in 25 states and Puerto Rico.

8. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

9. All of Plaintiff’s claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

10. This Court has subject matter jurisdiction over this action further to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because: (i) the amount in controversy exceeds \$5 million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiff Banks has different citizenship from Defendant.

11. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff’s and Class Members’ Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Defendant's Business

13. Azura is a Pennsylvania-based operator of 70 outpatient vascular centers and ambulatory surgery centers in 25 states and Puerto Rico.

14. As a condition of providing services, Azura requires its patients to entrust it with their Private Information.

15. Azura collects and maintains the Private Information of patients of its healthcare network, including but not limited to their:

- name,
- address,
- phone number and email address;
- date of birth;
- demographic information;
- Social Security number;
- financial information;
- information relating to individual medical history;
- information concerning an individual's doctor, nurse, or other medical providers;
- medication information;
- health insurance information;
- photo identification; and
- other information that Azura may deem necessary to provide its services.

16. Additionally, Azura may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), guarantors, close friends, and/or family members.

17. Because of the highly sensitive and personal nature of the information Azura acquires and stores with respect to its healthcare entities' patients and other individuals, Plaintiff and Class Members reasonably expect that Azura will, among other things: keep their Private Information confidential; comply with healthcare industry standards related to data security and Private Information; inform them of legal duties and comply with all federal and state laws

protecting their Private Information; only use and release their Private Information for reasons that relate to medical care and treatment; and provide adequate notice to them if their Private Information is disclosed without authorization.

18. Plaintiff and Class Members entrusted Azura with their Private Information but, contrary to Azura's duties, promises, and the reasonable expectations of Plaintiff and Class Members, Azura implemented substandard data security practices and failed to adhere to industry standard practices. Not only did Azura maintain inadequate security to protect its systems from infiltration by cybercriminals but it waited nearly two months to publicly disclose the Data Breach.

The Data Breach

19. According to the Notice Letter provided by Azura to Plaintiff and Class Members, Azura was subject to a cybersecurity attack beginning on or before September 27, 2023.

20. On November 9, 2023, Azura discovered that the Data Breach may have impacted Private Information stored in its systems and encrypted files.

21. In response, Azura stated that it "conducted incident response and recovery procedures, took steps to contain the incident, and investigated with the assistance of a third-party forensic firm."⁴

22. As a HIPAA covered entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Azura was aware and knew it had a duty to guard against.⁵

⁴ Notice Letter.

⁵ See, *HIPAA Notice of Privacy Practices*, FRESINIUS MEDICAL CARE, <https://fmcna.com/patient-care/vascular-access-care/#:~:text=A%20division%20of%20Fresenius%20Medical,as%20well%20as%20career%20development>. (last visited Feb. 28, 2024) ("Azura's Privacy Policy").

23. It is well-known that healthcare businesses such as Azura, that collect and store the confidential and private information, including protected health information, of hundreds of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

24. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and guarantors, including Plaintiff and Class Members.

25. Despite learning that the Data Breach compromised Private Information on November 9, 2023, Azura waited over two months following the completion of its investigation to notify the impacted individuals of the Data Breach and the need for them to protect themselves against fraud and identity theft. Azura was, of course, too late in the discovery and notification of the Data Breach.

26. Due to Azura's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

27. Azura had obligations created by the FTC Act, HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

28. Plaintiff and Class Members entrusted their Private Information to Azura with the reasonable expectation that Azura would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Azura's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and Class Members would not have allowed Azura or anyone in Azura's position to receive their Private Information had they known that Azura would fail to implement industry standard protections for that sensitive information.

31. As a result of Azura's negligent and wrongful conduct, Plaintiff's and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals. The unencrypted Private Information of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can now easily access the Private Information of Plaintiff and Class Members.

Defendant Knew or Should Have Known of the Risk Because Healthcare Entities In Possession of Private Information Are Particularly Susceptable to Cyberattacks

32. Azura knew at all relevant times that it was storing sensitive Private Information and that, as a result, its systems would be an attractive target for cybercriminals.

33. By obtaining, collecting, and storing Plaintiff's and class members' Private Information, Azura assumed express and implied legal duties, and knew or should have known that it was responsible for protecting Plaintiff's and class members Private Information from unauthorized disclosure.

34. Azura also knew that a breach of its systems and the information stored on them

would result in an increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

35. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

36. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

37. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁶

38. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."⁷

39. The healthcare sector suffered approximately 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.⁸

40. Healthcare related breaches, in particular, have continued to rapidly increase

⁶ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

⁷ *The Healthcare Industry is at Risk*, SWIVEL SECURE, <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/> (last visited Feb. 28, 2024).

⁸ Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, HEALTH IT SECURITY (July 19, 2022), <https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year>.

because electronic patient data is seen as a valuable asset. In fact, entities that store patient information “have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”⁹

41. Moreover, in light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

42. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

43. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

44. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the

⁹ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited on Feb. 28, 2024).

foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

45. Additionally, as companies became more dependent on computer systems to run their business,¹⁰ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹¹

46. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), amounting to potentially hundreds of thousands individuals’ detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

47. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

48. The ramifications of Defendant’s failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

49. As a healthcare services company in possession of current and former patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the

¹⁰ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last accessed Feb. 28, 2024).

¹¹ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022> (last accessed Feb. 28, 2024).

Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Azura Fails to Comply with FTC Guidelines

50. Azura is prohibited by the Federal Trade Commission Act (the “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

51. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

52. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.¹² The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

¹² *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).

someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

53. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. These FTC enforcement actions include actions against healthcare providers and partners like Azura. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”)

56. Azura failed to properly implement basic data security practices.

57. Azura’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Azura was at all times fully aware of the obligation to protect the Private

Information of its patients. Azura was also aware of the significant repercussions that would result from its failure to do so.

Azura Failed to Comply with HIPAA Guidelines

59. Defendant is a covered entity under HIPAA and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

60. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).¹³ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

61. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

62. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

63. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

64. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45

¹³ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

C.F.R. § 160.103.

65. HIPAA's Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

66. HIPAA also requires Defendant to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e).

67. Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

68. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

69. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable

delay and *in no case later than 60 days following discovery of the breach.*”¹⁴

70. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

71. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

72. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318.

73. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.¹⁵

74. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good

¹⁴ Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added). (last accessed Feb. 28, 2024).

¹⁵ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last accessed Feb. 28, 2024).

business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.¹⁶

Azura Failed to Comply with Industry Standards

75. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

76. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Azura, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

77. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

78. Azura failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are all established standards in reasonable

¹⁶ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last accessed Feb. 28, 2024).

cybersecurity readiness.

79. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Azura failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Azura Breached Its Duty to Safeguard Plaintiff's and the Class's Private Information

80. In addition to its obligations under federal and state laws, Azura owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Azura owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

81. Azura breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Azura's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect its patients' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- e. Failing to sufficiently train its employees and vendors regarding the proper handling of its patients' Private Information;

- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- g. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

82. Azura negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

83. Had Azura remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

84. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

85. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁷ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

¹⁷ 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number.”¹⁸

86. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁹

87. For example, PII can be sold at a price ranging from \$40 to \$200.²⁰ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²¹

88. Theft of PHI is gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”²²

89. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.²³

¹⁸ *Id.*

¹⁹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Sept. 13, 2023).

²⁰ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Sept. 13, 2023).

²¹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Sept. 13, 2023).

²² *What To Know About Medical Identity Theft*, Federal Trade Commission, (May 2021), available at <https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last visited Aug. 3, 2023).

²³ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed Feb. 28, 2024).

90. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁴

91. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

92. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

²⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed Feb. 28, 2024).

93. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

94. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁵

95. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”²⁶

96. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names, PHI, and Social Security numbers.

97. The fraudulent activity resulting from the Data Breach may not come to light for

²⁵ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed Feb. 28, 2024).

²⁶ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Feb. 28, 2024).

years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁷

98. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

99. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

100. Because a person’s identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

²⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Sept. 13, 2023).

101. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

102. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.²⁸

103. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

104. The development of “Fullz” packages means here that the stolen Private

²⁸ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-) (last visited on Sept. 13, 2023).

Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

105. The existence and prevalence of "Fullz" packages means that the Private Information stolen as a direct result of the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

106. Thus, even if certain information (such as driver's license numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

107. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Plaintiff & Class Members Suffered Harm as a Result of the Data Breach

108. Azura received Plaintiff's PII/PHI in connection with providing services to them. As discussed above, in requesting and maintaining Plaintiff's PII/PHI for business purposes, Azura expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's PII/PHI. Azura, however, did not take proper care of Plaintiff's PII/PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of Azura's inadequate data security measures.

109. On or around January 12, 2024, Azura sent Plaintiff a notice concerning the Data Breach. The letter stated that Azura experienced a cybersecurity attack and that the incident may have resulted in unauthorized access to Plaintiff's PII/PHI stored on Azura's systems.

110. To date, Defendant has not done anything to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

111. Defendant places the burden squarely on Plaintiff and Class Members by “encourag[ing]” them to expend their own time and money “to regularly review statements from their accounts and to periodically obtain their credit report from one or more of the national credit reporting companies.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

112. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

113. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant’s Notice Letter encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

114. For example, many victims of the Data Breach have suffered or will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts;
- f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come; and,
- g. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

115. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁹

116. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

²⁹ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁰

Diminution in Value of Private Information

117. PII and PHI are valuable property rights.³¹ Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

118. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³²

119. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{33, 34}

120. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁵

³⁰ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last accessed Feb. 28, 2024).

³¹ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

³² <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed Sept 13, 2023).

³³ <https://datacoup.com/> (last accessed Sept 13, 2023).

³⁴ <https://digi.me/what-is-digime/> (last accessed Sept 13, 2023).

³⁵ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last accessed Sep. 13, 2023).

121. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³⁶

122. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

123. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

124. Moreover, because this information is immutable, e.g., names, Social Security numbers, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

125. Thus, Plaintiff and Class Members may also incur out-of-pocket costs for protective

³⁶ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed Sep. 13, 2023).

measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information.

127. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Imminent and Continuing Risk of Future Fraud and Identity Theft

128. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

129. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

130. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

131. Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

132. Moreover, Plaintiff and Class Members have an interest in ensuring that their

Personal and Medical Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Personal and Medical Information is not accessible online and that access to such data is password protected.

Lost Benefit of the Bargain

133. Plaintiff greatly values his privacy, especially while receiving medical services and/or devices. Plaintiff and Class Members did not receive the full benefit of their bargain when paying for and/or entrusting their inherently valuable Private Information to Defendant in exchange for medical services, instead receiving services that were of a diminished value to those described in their agreements with Azura.

134. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for and/or entrusted their valuable Private Information for (which would have included adequate data security protection) and the services they actually received.

135. Plaintiff and Class Members would not have obtained services from Azura had they known that Azura failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

PLAINTIFF'S EXPERIENCE

Plaintiff Banks

136. Plaintiff Banks entrusted his Private Information to Defendant in order to receive medical care from one of Azura's affiliated medical groups.

137. Plaintiff Banks's Private Information was in the possession and control of

Defendant at the time of the Data Breach.

138. Plaintiff Banks provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

139. On or around January 12, 2024, Defendant notified Plaintiff Banks that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

140. Plaintiff Banks is very careful about sharing his sensitive Private Information. Plaintiff Banks has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

141. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

142. As a result of the Data Breach, Plaintiff Banks spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred and freezing his own credit. This time has been lost forever and cannot be recaptured.

143. Even with the best response, the harm caused to Plaintiff Banks cannot be undone.

144. Plaintiff Banks suffered actual injury in the form of unauthorized charges made by an unknown party to his personal debit card on or around November 27, 2023. Plaintiff spent time mitigating the effects of this unauthorized charges to his debit card, namely taking the time to dispute the unauthorized charges with Plaintiff's bank, as well as going through the process to order a replacement debit card.

145. Plaintiff Banks suffered additional injury in the form of damages to and diminution

in the value of his Private Information—a form of intangible property that Plaintiff Banks entrusted to Defendant, which was compromised in and as a result of the Data Breach.

146. Plaintiff Banks suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

147. Defendant admits that Plaintiff Banks’s Private Information was exfiltrated by criminal third-parties. Thus, Plaintiff Banks’s and Class Members’ information is already being misused by cybercriminals.

148. Plaintiff Banks has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

149. Plaintiff Banks has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain backed up in Defendant’s possession, is protected, and safeguarded from future breaches.

CLASS ALLEGATIONS

150. Plaintiff brings this action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure. Plaintiff intend to seek certification of the Nationwide Class or, in the alternative, the Virginia, New Jersey and Pennsylvania Subclasses set forth below.

151. The **Nationwide Class** that Plaintiff seek to represent is defined as follows:

All individuals residing in the United States whose Private Information was compromised in the Data Breach, including all who received Notice of the Data Breach (the “Nationwide Class” or “Class”).

152. The **Illinois Subclass** that Plaintiff Banks seeks to represent is defined as follows:

All individuals residing in the state of Illinois whose Private Information was compromised in the Data Breach, including all who received Notice of the Data Breach (the “Illinois

Subclass”).

153. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

154. Plaintiff reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

155. **Numerosity**, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. According to the U.S. Department of Health and Human Services, the Data Breach compromised the information of about 348,000 people.³⁷ The Class Members are identifiable within Defendant’s records inasmuch as Defendant has already provided them with notification of the breach.

156. **Commonality**, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact are common to the Class Members and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

³⁷ *Azura Vascular Care reports data breach, exposing 348k patients*, (Feb. 7, 2024), available: https://beyondmachines.net/event_details/azura-vascular-care-reports-data-breach-exposing-348k-patients-v-y-m-o-9.

- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. When Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

157. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because they all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

158. **Conduct Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

159. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff have retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

160. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3):** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

161. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

162. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

163. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

164. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may

continue to act unlawfully as set forth in this complaint.

165. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

166. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and,
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
*(On Behalf of Plaintiff and the Nationwide
Class or, Alternatively, the Illinois Subclass)*

167. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

168. Azura collected the Private Information of Plaintiff and Class Members in the ordinary course of providing services and/or employment to Plaintiff and Class Members.

169. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Azura owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Azura's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

170. Azura owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

171. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that Azura was aware, or should have been aware, could be injured by inadequate data security measures.

172. Azura owed numerous duties to Plaintiff and the Class, including the following:

- To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

- To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

173. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Azura knew or should have known that, given its repository of a host of Private Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Azura had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably to safeguard the Private Information.

174. Azura's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Azura and patients. Azura was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

175. Azura's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Azura is bound by industry standards to protect confidential Private Information.

176. Azura breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Azura includes, but is not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Failing to have in place mitigation policies and procedures;
- e. Allowing unauthorized access to Class Members' Private Information;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

177. It was foreseeable that Azura's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

178. Azura's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

179. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

180. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered damages as alleged above.

181. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

182. Plaintiff and Class Members are also entitled to injunctive relief requiring Azura to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
***(On Behalf of Plaintiff and the Nationwide Class or, Alternatively,
the Illinois Subclass)***

183. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

184. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Azura had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

185. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Azura also had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

186. Pursuant to HIPAA, Azura had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

187. Azura breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

188. Plaintiff and Class Members were within the Class of Persons that HIPAA and the FTC Act are intended to protect and the harm resulting from the Data Breach is the type of injury against which the statutes are intended to guard.

189. Azura's failure to comply with applicable laws and regulations constitutes negligence per se.

190. But for Azura's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

191. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Azura's breach of its duties. Azura knew or should have known that it was failing to meet its duties, and that P Azura's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

192. As a direct and proximate result of Azura's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
***(On Behalf of Plaintiff and the Nationwide Class or, Alternatively,
the Illinois Subclass)***

193. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

194. Plaintiff and the Class Members entered into implied contracts with Azura under which Azura agreed to take reasonable measures to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

195. Plaintiff and the Class Members were required to and delivered their Private Information to Azura as part of the process of obtaining services provided by Azura. Plaintiff and Class Members paid money, or money was paid on their behalf, to Azura in exchange for services, or as a condition of their employment with a medical group affiliated with Azura.

196. Azura solicited, offered, and invited Class Members to provide their Private Information as part of Azura's regular business practices. Plaintiff and Class Members accepted Azura's offers and provided their Private Information to Azura.

197. Azura accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services for Plaintiff and Class Members.

198. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Azura whereby Azura became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

199. In delivering their Private Information to Azura and paying for healthcare services, Plaintiff and Class Members intended and understood that Azura would adequately safeguard the data as part of that service.

200. Upon information and belief, in its written policies, Azura expressly and impliedly promised to Plaintiff and Class Members that they would only disclose protected information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

201. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

202. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

203. Plaintiff and the Class Members would not have entrusted their Private Information to Azura in the absence of such an implied contract.

204. Had Azura disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Private Information to Azura.

205. Azura recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

206. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Azura.

207. Azura breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

208. As a direct and proximate result of Azura's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
BREACH OF FIDUCIARY DUTY
***(On Behalf of Plaintiff and the Nationwide Class or, Alternatively,
the Illinois Subclass)***

209. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

210. Plaintiff brings this Count on behalf of himself and on behalf of the Nationwide Class.

211. Defendant accepted and used Plaintiff's and Class Members' Private Information for its own pecuniary benefit and accepted the Private Information with full knowledge of the need to maintain it as confidential, the need to implement appropriate data security measures, and the significant harm that would result to Plaintiff and Class Members if the confidentiality of their Private Information was breached.

212. Defendant as their healthcare provider was in a superior position of trust and authority to Plaintiff and Class Members.

213. Plaintiff and Class Members had no way to ensure that Defendant's data security measures were adequate and no way to influence or verify the integrity of Defendant's data security posture.

214. Defendant knew that it was in an exclusive position to safeguard Plaintiff's and Class Members' Private Information from the foreseeable threat of a cyberattack and understood Plaintiff's and Class Members' expectations that it would safeguard their Private Information.

215. In light of the special relationship between Azura and Plaintiff and Class Members, Azura became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private

Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Azura do store.

216. Azura had a fiduciary duty to act for the benefit of Plaintiff and Class Members, in particular, to keep secure and confidential their Private Information.

217. Azura breached its fiduciary duty to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

218. Azura breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

219. Azura breached its fiduciary duty owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

220. Azura breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

221. As a direct and proximate result of Azura's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Azura's possession and is subject to further unauthorized

disclosures so long as Azura fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Azura's services they received.

222. As a direct and proximate result of Azura's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
***(On Behalf of Plaintiff and the Nationwide Class or, Alternatively,
the Illinois Subclass)***

223. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

224. This count is pleaded in the alternative to the above contract-based claims pursuant to Fed. R. Civ. P. 8.

225. Upon information and belief, Azura funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

226. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Azura.

227. Plaintiff and Class Members conferred a monetary benefit on Azura. Specifically, they purchased goods and services from Azura and/or its agents and in so doing provided Azura with their Private Information. In exchange, Plaintiff and Class Members should have received from Azura the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

228. Azura knew that Plaintiff and Class Members conferred a benefit which Azura accepted. Azura profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

229. Plaintiff and Class Members conferred a monetary benefit on Azura, by paying Azura as part of rendering medical services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Private Information, and by providing Azura with their valuable Personal Information.

230. Azura was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Azura instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Azura's failure to provide the requisite security.

231. Under the principles of equity and good conscience, Azura should not be permitted to retain the money and valuable Private Information belonging to Plaintiff and Class Members, because Azura failed to implement appropriate data management and security measures that are mandated by industry standards.

232. Azura acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

233. If Plaintiff and Class Members knew that Azura had not secured their Private Information, they would not have agreed to provide their Private Information to Azura.

234. Plaintiff and Class Members have no adequate remedy at law.

235. As a direct and proximate result of Azura's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Azura's possession and is subject to further unauthorized disclosures so long as Azura fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

236. As a direct and proximate result of Azura's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

237. Azura should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Azura should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Azura's services.

COUNT VI

**Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act,
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff Banks and the Illinois Class)**

238. Plaintiff Banks realleges and incorporates by reference all preceding allegations as though fully set forth herein.

239. Plaintiff Banks brings this cause of action individually and on behalf of the members of the Illinois Subclass.

240. The Illinois Consumer Fraud and Deceptive Business Practices Act was created to protect Illinois consumers from deceptive and unfair business practices.

241. Azura's conduct described herein constitutes use or employment of deception, false promise, misrepresentation, unfair practice and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of medical services, in trade or commerce in Illinois, with the intention that Plaintiff and Illinois Subclass members would rely on such conduct in deciding to give their Private Information to Azura in exchange for receiving medical services, making it unlawful under 815 Ill. Comp. Stat. Ann. §505/1, *et seq.*

242. Plaintiff and Illinois Subclass members relied on the material representations made by Azura about its data security practices and provided their Private Information with the understanding that Azura would safeguard this Private Information. Plaintiffs and Class Members suffered ascertainable losses of money or property as the result of the use or employment of a method, act or practice declared unlawful by 815 Ill. Comp. Stat. Ann. §505/1, *et seq.* Plaintiff and Illinois Subclass members acted as reasonable consumers would have acted under the circumstances, and Azura's unlawful conduct would cause reasonable persons to enter into the transactions (providing Private Information in exchange for medical services) that resulted in the damages.

243. Accordingly, pursuant to 815 Ill. Comp. Stat. Ann. §505/1, *et seq.*, Plaintiffs and Illinois Subclass members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. In addition, given the nature of Azura's conduct, Plaintiffs and Illinois Subclass members are entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from Azura's unlawful conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment in their favor and against Azura as follows:

- A. For an Order certifying the Nationwide Class and state subclass and appointing Plaintiff and their Counsel to represent such Classes;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against

the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and

Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: March 20, 2024

Respectfully Submitted,



/s/

Benjamin F. Johns (PA Bar 201373)
Samantha E. Holbrook (PA Bar 311829)
Andrea L. Bonner (PA Bar 332945)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Fax: (856) 210-9088
bjohns@shublawayers.com
sholbrook@shublawayers.com
abonner@shublawayers.com

Attorneys for Plaintiffs